

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-312382

(43)Date of publication of application : 07.11.2000

(51)Int.Cl.

H04Q 7/38

G06F 1/00

H04L 9/32

(21)Application number : 11-119186

(71)Applicant : HITACHI LTD

(22)Date of filing : 27.04.1999

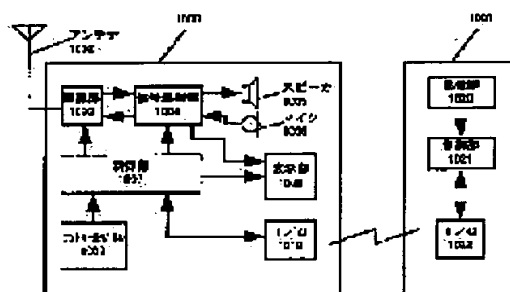
(72)Inventor : YAMAMOTO NAOKI
SHIMIZU HIROSHI

(54) MOBILE TERMINAL

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent illegal use of a mobile terminal by easily changing the right of a user of a mobile terminal.

SOLUTION: A user carries a contactless information communication unit 1001 that stores a personal user ID and uses a contactless IC chip as a method for accessing ID information from the outside, and makes communication with a mobile terminal 1000. Thus, the communication unit 1001 transfers the ID information to a user ID mobile terminal where a person is authenticated, and the user ID mobile terminal is allowed to utilize part or all of functions of its so long as the user ID mobile terminal is found to have the right of utilizing various information communication services by receiving the ID information.



LEGAL STATUS

[Date of request for examination] 22.09.2003

[Date of sending the examiner's decision of rejection] 28.06.2005

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of

rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-312382

(P2000-312382A)

(43) 公開日 平成12年11月7日 (2000.11.7)

(51) Int. CL ⁷	識別記号	F I	テ-マコード ⁶ (参考)
H 0 4 Q 7/38		H 0 4 B 7/25	1 0 9 S 5 J 1 0 4
G 0 6 F 1/00	3 7 0	G 0 6 F 1/00	3 7 0 F 5 K 0 6 7
			3 7 0 E
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 A
			6 7 3 E
審査請求 未請求 請求項の数 5 O L (全 6 頁)			

(21) 出願番号 特願平11-119186

(22) 出願日 平成11年4月27日 (1999.4.27)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 山本 直樹

神奈川県横浜市戸塚区吉田町292番地株式会社日立製作所マルチメディアシステム開発本部内

(72) 発明者 清水 宏

神奈川県横浜市戸塚区吉田町292番地株式会社日立製作所マルチメディアシステム開発本部内

(74) 代理人 100075086

弁護士 作田 康夫

最終頁に続く

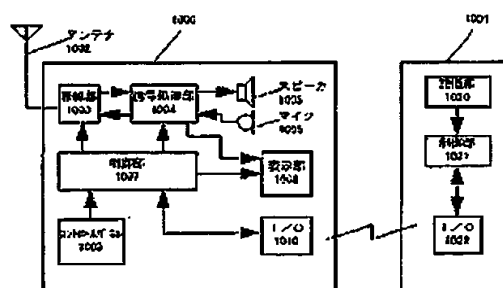
(54) 【発明の名称】 携帯端末装置

(57) 【要約】

【課題】携帯端末装置の利用権利の変更を容易にし、不正使用を防止する。

【解決手段】個人のユーザIDを記憶し、外部から同情報にアクセスする方法として非接触ICチップを用いた非接触情報通信装置1001をユーザが携帯し、携帯端末装置1000と通信する事により、ユーザID携帯端末装置に転送して個人認証を行い、各種情報通信サービスを利用する権利があると認識した場合に限り、該携帯端末装置の有する機能の一部若しくは全てを利用可能とする。

図 1



(2)

特開2000-312382

1

【特許請求の範囲】

【請求項1】通信により、通話、データ送受信等のサービスを有料にて行う携帯端末装置において、ユーザID記憶手段と通信手段を有し、該携帯端末装置と非接触にて情報の送受信を行う第1の非接触情報通信手段と、該第1の非接触情報通信手段と情報の送受信を行う第2の非接触情報通信手段を該携帯端末装置内に具備し、該携帯端末装置が該ユーザIDを認識可能状態であるときのみ、該第1の非接触情報通信手段を所持するユーザに、該サービスの利用権を与え、共に、利用したサービスに応じた課金を行う機能を有することを特徴とする携帯端末装置。

【請求項2】通信により、通話、データ送受信等のサービスを有料にて行う携帯端末装置において、ユーザID記憶手段と該サービスの利用履歴及び課金情報等を記憶するサービス履歴記憶手段と通信手段を有し、該携帯端末装置と非接触にて情報の送受信を行う第1の非接触情報通信手段と、該第1の非接触情報通信手段と情報の送受信を行う第2の非接触情報通信手段を該携帯端末装置内に具備し、該携帯端末装置が該ユーザIDを認識可能状態であるときのみ、該第1の非接触情報通信手段を所持するユーザに、該サービスの利用権を与え、共に、利用したサービスに応じた課金を行い、利用したサービスの履歴及び課金状況を第1の非接触情報通信手段のサービス履歴記憶手段に記憶する機能を有することを特徴とする携帯端末装置。

【請求項3】請求項1または2に記載の携帯端末装置において、発信開始毎に該第1の非接触情報通信手段よりユーザIDを読み取り個人認証を自動的に行うことを特徴とする携帯端末装置。

【請求項4】請求項1または2に記載の携帯端末装置において、待ち受け状態においては定期的にユーザIDを読み取り個人認証を行うことを特徴とする携帯端末装置。

【請求項5】請求項1または2に記載の携帯端末装置において、該携帯端末装置にSW操作による個人認証開始手段と、個人認証確認手段を設け、ユーザのSW操作によりユーザIDを読み取り個人認証を行うと共に、該個人認証結果をユーザが確認できる機能を有する事を特徴とする携帯端末装置。

【発明の詳細な説明】

【発明の属する技術分野】本発明は、個人認証を行うための装置に係わり、特に携帯端末装置のサービス利用許可を行うための、認証装置に係わる。

【従来の技術】日経エレクトロニクス1999年3月22日号P123-140に記載されているように、携帯電話を代表とする携帯情報端末装置は「通話」のみならず「オンライン・バンキング」「情報提供サービス」「電子メール」「インターネット接続」等のサービスを展開し、多機能化が進んでいる。

2

【発明が解決しようとする課題】しかし、携帯端末装置には電源切れ、携帯忘れ、紛失や故障による不慮の事故等により使用できない場合があるばかりでなく、他人による不正使用の可能性が拭き切れない。また、所有者の許可を得て他人の携帯端末装置を借用する場合に於いては、利用したサービスの使用料金がその携帯端末装置の所有者に課金されることになり、気軽に貸し借りができる環境ではない。

【課題を解決するための手段】この問題点を解決するために本発明では、個人のユーザIDを記憶し、外部から同情報にアクセスする方法として非接触ICチップを用いた非接触情報通信手段を用い、これをカード、指輪、時計、イヤリング、ネックレス、ペンダント等の身に付け易いものに組み込む事により、常にユーザが携帯できるようにする。更に、携帯端末装置にも非接触ICチップを用いた非接触情報通信手段を具備する。携帯端末装置は、必要に応じて上記非接触情報通信手段間の通信によりユーザIDを読み出し、各種情報通信サービスを利用する権利があると認識した場合に限り、該携帯端末装置の有する機能の一部若しくは全てを利用可能とする。

【発明の実施の形態】以下、本発明による非接触情報通信を用いた個人認証機能を有する携帯端末装置の実施の形態の具体例を図を用いて説明する。図1は、本発明による携帯端末装置及び個人認証用ICカードのシステムブロック図である。1000は携帯端末装置、1001は個人認証用ICカードである。携帯端末装置1000は個人認証用の非接触情報通信を行うI/O1010を除けば公知の技術により構成された携帯電話等の携帯端末装置である。携帯端末装置1000は個人認証用ICカード1001が接近し通信可能領域に入ると、非接触情報通信を行うI/O1010により個人認証用ICカードと通信を開始する。個人認証用ICカード1001は、ユーザIDを記憶している記憶部1020、通信によりデータの入出力を行うI/O1022、データの送受信等を制御する制御部1021とから成り、制御部1021はユーザIDをI/O1022により携帯端末装置1000のI/O1010に転送する。尚この個人認証用ICカード1001の電源は、電磁結合方式等により通信相手である携帯端末装置1000から供給してもらってもよく、個人認証用ICカード1001自身にボタン型電池等を内蔵してもよい。制御部1007は、サービス提供者により予め登録されている携帯端末装置1000固有の機器IDと個人認証用ICカード1001より受信したユーザIDを無線部1003に送りアンテナ1002を通じて図示しないサービス提供局と通信を行うことで、サービス利用許可となる個人認証を受ける。この後、ユーザがコントロールパネル1009を操作することにより、音声であればマイク1006、スピーカ1005、文字・画像であれば表示部1008を入出力デバイスとして、信号処理部1004、無線部1003、アンテナ1002を介して図示しないサービス提供局と通信を行うことにより、通話、オンライン・バンキング、情報提供サービ

(3)

特開2000-312382

3

ス、電子メール、インターネット等のサービスを利用可能となる。上記ユーザIDにはサービス提供者との契約により登録されている電話番号、利用可能サービスの種類等が含まれており、サービス提供者は契約に応じたサービスの供給を行うと共に、利用したサービスの代金を個人認証用ICカードの所有者であるユーザに課金する。図2に、上記個人承認が完了したときの表示部1008の表示画面の一例を示す。コントロールパネル1009にある図示しない個人認証確認SWをユーザが操作するか、個人認証が完了した直後の数秒間に、表示部1008は表示画面2000を出力する。表示画面2000には、ユーザ名2001、サービス提供者と契約により取得した電話番号2002及び利用可能サービス一覧2003等が表示され、利用状況の確認ができる。図3に、本実施例の利用形態の概念図を示す。ユーザ3000は個人認証用ICカード1001をポケット等に入れて常に携帯する。ユーザ3000が携帯端末装置1000を電源を入れた状態で、(A)に示す様に個人認証用ICカード1001との通信可能領域に携帯することで個人認証用ICカード1001に記憶されているユーザIDによる上記個人認証処理を開始され、ユーザ3000は携帯端末装置1000を用いてサービスを利用できる。ここで、携帯端末装置1000は上記個人認証処理を定期的に行う処理を行う事で、置き忘れ、紛失等により(B)に示す様に通信可能領域から外れた場合には携帯端末装置1000はユーザ3000のユーザIDでのサービス利用ができなくなり、不正使用は不可能となる。ここで、個人のユーザIDを記憶し、外部から同情報にアクセスする方法として非接触ICチップを用いた非接触情報通信手段の形状は、個人認証用ICカード1001のようなカード形状のものに限らず、指輪、時計、イヤリング、ネックレス、ペンダント等の身に付け易い形状であれば同様の効果が得られる事は言うまでもない。図4は、本発明による別の実施形態の形態を説明するための携帯端末装置及び個人認証用ICカードのシステムブロック図である。同図において、個人認証用ICカード5000に書き込み可能な記憶部5001を新たに追加した事を除けば図1と同様の構成であり、以下の処理を除けば同じ処理を行う。以下、実施例における新たな処理を説明する。携帯端末装置1000は個人認証用ICカード4000との間で非接触通信により上記個人認証処理を行った後、通話、オンライン・バンキング、情報提供サービス、電子メール、インターネット等のサービスを実行する。このとき利用したサービスの内容、実行した日時、課金されるべき利用金額等のサービス利用状況データを、I/O1010を介して個人認証用ICカード4000に転送する。個人認証用ICカード4000はI/O1022を通じて上記サービス利用状況データを受信した後、制御部1021は同サービス利用状況データを記憶部4004に記憶する。同処理は、ユーザが携帯端末装置1000と同じ能力を持つ種々の携帯端末装置を用いてサービスを利用する毎に実行されサービス利用状況データの更

4

新を行う。しかる後、携帯端末装置1000にあるコントロールパネル1009の図示しないサービス利用状況確認SWをユーザが操作することで、個人認証用ICカード4000と通信を行い記憶部4004にあるサービス利用状況データを読み出して表示部1008に出力する。図5に、上記サービス利用状況確認時に表示部1008が出力する表示画面の一例を示す。ユーザが過去のサービス利用状況を確認したい場合、上記したサービス利用状況確認SWの操作により、表示部1008は表示画面6000を出力する。表示画面6000には、ユーザ名2001、サービス提供者と契約により取得した電話番号2002及び利用可能サービス一覧2003等が表示されており、各項目を選択することによりサービス毎の利用履歴を表示できる。表示画面5001はユーザが表示画面5000を見て「通話」の利用履歴をコントロールパネル1009により選択した時の表示画面である。表示画面5001には、通話した日時、相手の電話番号、利用料金等が表示される。これらの情報と、サービス業者から別途送付される請求書等の課金情報と照らし合わせる事により不正利用等の存在を確認することもできる。

【発明の効果】以上のような本発明により、ユーザは携帯端末装置の利用可能とするための個人承認を容易に行う事ができ、携帯端末装置使用の自由度を向上する効果がある。また、個人承認処理を定期的に行うことで、置き忘れ、紛失時の他人による不正使用を防止する効果もある。

【図面の簡単な説明】

【図1】本発明による第1の実施形態の形態携帯端末装置及び個人認証用ICカードのシステムブロック図である。

【図2】個人承認が完了したときの表示画面の具体例である。

【図3】本発明の利用形態の概念図である。

【図4】本発明による第2の実施形態の形態を説明するための携帯端末装置及び個人認証用ICカードのシステムブロック図である。

【図5】サービス利用状況確認時の表示画面の具体例である。

【符号の説明】

1000 … 携帯端末装置
1001 … 個人認証用ICカード
1002 … アンテナ
1003 … 無線部
1004 … 信号処理部
1005 … スピーカ
1006 … マイク
1007, 1021 … 制御部
1008 … 表示部
1009 … コントロールパネル
1010, 1022 … I/O
1020 … 記憶部
2000 … 表示画面

(4) 特開 2000-312382

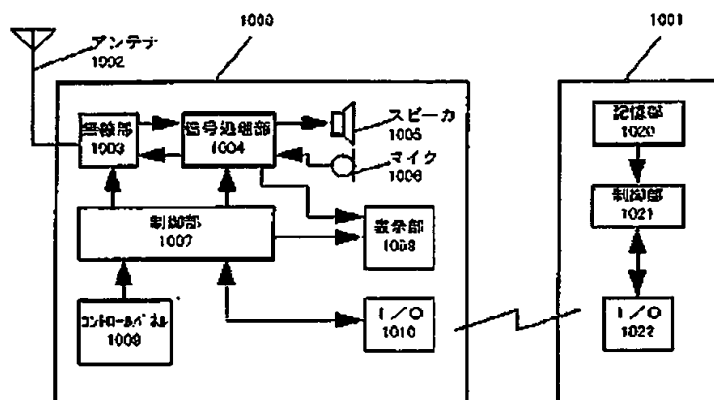
2001 ... ユーザ名
2002 ... 電話番号
2003 ... サービス一覧
3000 ... ユーザ

* 4000 ... 個人認証用 IC カード
4001 ... 記憶部
5000, 5001 ... 表示画面

*

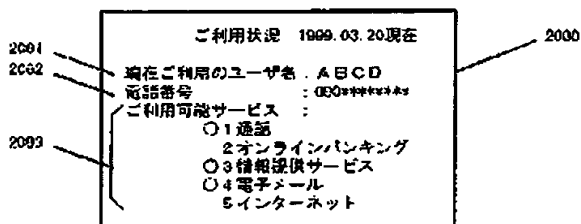
【図 1】

図 1



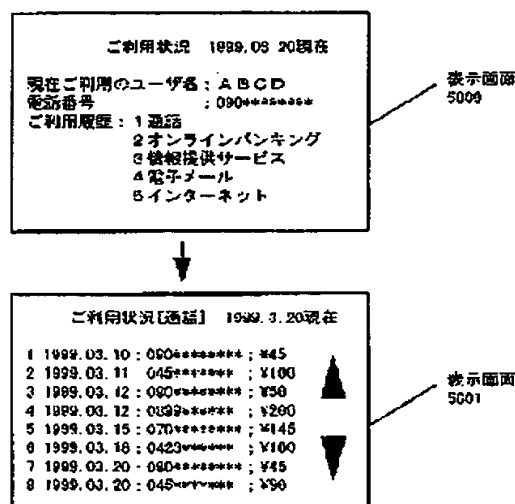
【図 2】

図 2



【図 5】

図 5

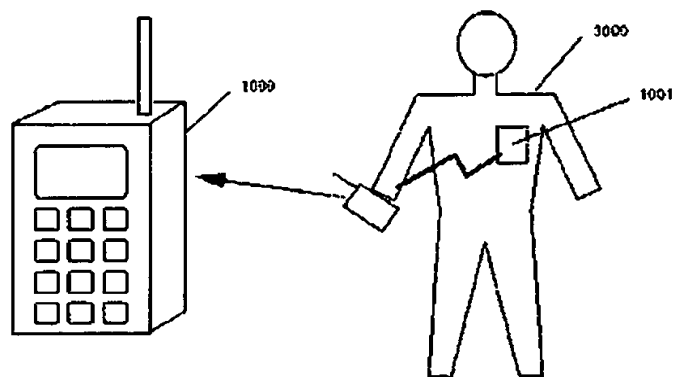


(5)

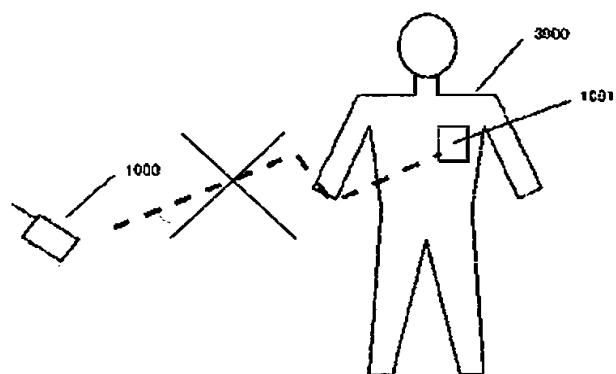
特開2000-312382

【図3】

図3



(A)



(B)